Communiqués et discours

Discours

INTERVENTION DE LA PRÉSIDENTE
DEVANT LA COMMISSION DE L'ÉCONOMIE ET DU TRAVAIL
CONCERNANT L'AVANT-PROJET DE LOI SUR LA NORMALISATION JURIDIQUE DES NOUVELLES TECHNOLOGIES DE L'INFORMATION

29 août 2000

INTRODUCTION

Je tiens d'abord à remercier la Commission de l'économie et du travail d'avoir invité la Commission d'accès à l'information dès le début de la consultation générale sur l'avant-projet de loi sur la normalisation juridique des nouvelles technologies de l'information.

Permettez-moi maintenant de vous présenter les personnes qui m'accompagnent : M^e^ André Ouimet, secrétaire de la Commission et directeur des services juridiques et M. Robert Parent, directeur par intérim de l'analyse et de l'évaluation.

La Commission se réjouit du dépôt de cet avant-projet de loi. La sécurité juridique des communications sur l'inforoute représente actuellement tout un défi et les enjeux en cause sont importants. Ils recoupent autant divers aspects de la vie quotidienne des citoyens et citoyennes, que des conditions nécessaires à la poursuite des échanges économiques pour des industries traditionnelles et pour des industries qui se créent actuellement dans ce nouveau contexte technologique. À nos yeux, l'avant-projet est innovateur et audacieux.

La Commission félicite le gouvernement de cette initiative qui a le mérite notamment d'être fidèle à l'héritage du droit civil québécois. Il a également le mérite d'assurer une pérennité aux principes juridiques qui y sont énoncés, permettant ainsi à ces principes de s'adapter à l'évolution technologique.

La Commission a déposé un avis sur l'avant-projet de loi sur la normalisation juridique des nouvelles technologies de l'information qui explique en détail notre position.

Cet avant-projet, nous l'avons dit, est important. La Commission l'a étudié à la lumière des principes qui constituent le fondement même de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (la Loi sur l'accès) et la *Loi sur la protection des renseignements personnels dans le secteur privé* (la Loi sur le secteur privé). Du reste, ces principes se retrouvent dans l'ensemble des lois qui visent à protéger les données nominatives dans un nombre toujours plus grand de pays à travers le monde. Il m'apparaît important de rappeler les principes qui sont en cause aujourd'hui.

Il s'agit de la cueillette, de la conservation, de l'utilisation, de la communication et de

2008-05704/

l'accès aux renseignements personnels par la personne concernée.

Un mot sur chacun de ces principes qui cachent, disons-le, des réalités fort simples :

- la cueillette: un organisme public ou une entreprise ne peut recueillir que les renseignements qui sont nécessaires à ses attributions ou à l'objet de ses dossiers;
- la conservation: les renseignements personnels doivent être conservés de façon à en assurer le caractère confidentiel;
- l'utilisation: dans un organisme ou une entreprise, l'utilisation de renseignements personnels est réservée aux seules personnes qui en ont besoin dans l'exercice de leurs fonctions;
- communication: aucun renseignement personnel ne peut être communiqué, sauf exception, sans le consentement de la personne concernée;
- accès : chaque individu possède un droit d'accès aux renseignements qui le concerne.

La Commission n'entend donc pas commenter tous les aspects de l'avant-projet de loi, mais limiter ses commentaires à son domaine de compétence : la protection des renseignements personnels.

Disons-le tout de suite, à cet égard l'avant-projet de loi respecte, de façon générale, les principes que je viens de vous décrire.

Toutefois, cet avant-projet de loi soulève quand même certaines interrogations et amène la Commission à formuler des commentaires.

Avant de ce faire, il nous faut cependant rappeler une distinction importante entre les termes " sécurité " et " confidentialité ".

I. CONFIDENTIALITÉ ET SÉCURITÉ : DEUX NOTIONS DISTINCTES

En effet, comme le souligne l'avis de la Commission, la sécurité et la confidentialité sont deux notions qui visent des finalités fort différentes. La notion de confidentialité réfère à un ensemble de règles inscrites dans la législation qui couvrent toutes les phases de traitement de l'information de la cueillette à la communication, en passant par la détention, l'utilisation et la communication.

Un organisme public ou une entreprise peut avoir pris les moyens les plus perfectionnés sur le plan technologique pour assurer la sécurité d'une transmission de renseignement personnel, mais si le destinataire n'est pas légalement autorisé à recevoir une telle communication, il y aura un réel bris de confidentialité.

Par exemple, serait illégale la communication d'un renseignement médical concernant une personne à une compagnie d'assurance si la personne concernée n'y a pas consenti. Même si l'organisme qui communique ce renseignement a pris toutes les mesures de sécurité requises pour la transmission de ces renseignements, il y aura tout de même illégalité. L'organisme ou l'entreprise doit se poser la question préalable suivante : avons-nous le droit de communiquer ou de recueillir un tel renseignement ?

La notion sécurité n'est qu'un moyen qui a pour but de garantir le caractère confidentiel d'un renseignement.

À cet égard, la Commission souligne dans son avis que l'avant-projet de loi réussit à bien distinguer ces deux notions.

La personne qui communique un renseignement confidentiel doit s'assurer, dans un premier temps, que le destinataire a droit aux informations (art. 37).

Ces notions étant précisées, j'entends maintenant vous faire part de commentaires particuliers.

II. LES COMMENTAIRES DE LA COMMISSION

II.1 Le contrôle de l'accès aux renseignements personnels qui ont un caractère public

L'article 27 de l'avant-projet de loi vise à restreindre l'accès aux renseignements personnels qui ont un caractère public. Cette disposition aurait un impact majeur et important sur l'article 55 de la Loi sur l'accès. Ce dernier article précise qu'un renseignement personnel qui a un caractère public en vertu de la loi n'est pas confidentiel.

Cet article 27 propose une piste de solution intéressante à un problème longuement décrit dans le Rapport quinquennal de la Commission de 1997.

Ainsi, chaque fois qu'une disposition législative prévoit le caractère public de renseignements personnels, une fin bien précise est visée. Ainsi, le caractère public des renseignements consignés dans un rôle d'évaluation permet aux citoyens de connaître, aux fins de comparaison, pour l'une ou l'autre des unités d'évaluation, l'identité et l'adresse du propriétaire ainsi que la valeur de ses immeubles.

Consignés sur un support papier, ces renseignements seront accessibles aux personnes qui prendront le temps de se déplacer pour les consulter ou qui formuleront une demande écrite pour les obtenir. Ces modes d'accès qui, règle générale, étaient les seuls possibles lorsque les lois ont reconnu un caractère public à certains renseignements, garantissent le respect de l'objectif visé par la reconnaissance de ce caractère public. Par contre, lorsqu'ils deviennent facilement accessibles par des moyens technologiques, on peut se demander si une communication massive de renseignements personnels ne vient pas détourner ou contourner cet objectif. L'obtention massive de renseignements personnels à caractère public respecte rarement la finalité visée par le législateur et ouvre facilement la voie à des activités de nature commerciale ou de sollicitation.

L'article 27 limite la communication des renseignements personnels qui ont un caractère public lorsque l'accès à ces renseignements est rendu possible, par exemple, sur un site internet d'un organisme public ou d'une entreprise du secteur privé. Dans une telle situation, l'utilisation d'une fonction de recherche extensive peut en effet être contrôlée.

La Commission se réjouit de cette initiative qui, de fait, constituerait un progrès quant à la protection des renseignements personnels.

Cependant, la Commission entend discuter plus largement de toute cette question au moment des audiences de la Commission parlementaire qui entreprendra ses travaux

sur la révision de la *Loi sur l'accès* à compter du 12 septembre prochain

II.2 Le lien entre les personnes et les documents technologiques

L'identification des personnes qui utilise la technologie dans ses communications est au coeur de nos préoccupations comme société (articles 41 à 44). Selon l'avant-projet de loi, la vérification de l'identité d'une personne pourra se faire au moyen de divers documents. Encore une fois, et la Commission l'apprécie, l'avant-projet de loi maintient une ligne de neutralité technologique.

Ainsi, l'identité d'une personne pourra être établie en se référant aux registres prévus au Code civil du Québec ou à la Loi sur la publicité légale des entreprises individuelles, des sociétés et des personnes morales. La vérification de l'identité d'une personne pourra également être établie à partir de caractéristiques, connaissances ou objets qu'elle présente ou possède. Un document technologique pourra également servir à cette identification.

La Commission tient à rappeler que certaines lois interdisent l'utilisation d'identifiants créés à des fins précises. Ainsi, par exemple, la *Loi sur l'assurance maladie* stipule que la carte d'assurance maladie ne peut être exigée que pour vérifier l'identité et l'admissibilité d'une personne qui requiert des soins ou services de santé. L'obligation d'exhiber son permis de conduire est également strictement encadrée par la législation québécoise. Respectant ce principe de la spécificité des identifiants, la Commission croit qu'il serait approprié de préciser que la vérification de l'identité d'une personne doit se faire dans le respect de la loi.

La Commission croit que les articles 45 et 46 qui visent, entre autres, à maintenir confidentiels certains renseignements nécessaires à l'établissement de l'identité d'une personne, sont des articles très importants au regard de la protection des renseignements personnels. Ainsi, l'article 45 prévoit que les renseignements confidentiels que contient un document qui sert à confirmer l'identité d'une personne doivent être protégés. Quant à l'article 46, il précise que le document technologique qui sert de preuve d'identité doit être protégé contre l'interception lorsque sa conservation ou sa transmission sur un réseau de communication rend possible l'usurpation de l'identité de la personne visée par ce document. De plus, ajoute ce même article, la confidentialité de ce document doit être protégée, le cas échéant, et sa consultation doit être journalisée. La Commission comprend que cela veut dire par exemple que lors d'une transaction entre un client et une entreprise, cette dernière devra prendre des mesures spécifiques pour assurer la confidentialité des renseignements que fournit le client pour ainsi le prémunir contre une usurpation de son identité.

L'ensemble de ces mesures, estime la Commission, facilitera grandement les échanges entre le citoyen et l'administration publique et entre ce même citoyen et les entreprises avec lesquelles il fait affaire. En effet, les règles relatives à la fiabilité des documents et à l'identification des personnes éviteront que des personnes non autorisées puissent avoir accès à des renseignements personnels lorsque les nouvelles technologies de l'information serviront de base aux communications. Ainsi, l'usurpation de l'identité sera rendue plus difficile et l'exactitude des renseignements échangés sera mieux assurée.

II.3 LA BIOMÉTRIE COMME OUTIL D'IDENTIFICATION

L'article 50 de l'avant-projet de loi ouvre la voie à la vérification ou à la confirmation de l'identité d'une personne au moyen d'un procédé permettant de saisir des caractéristiques ou des mesures biométriques comme par exemple, les empreintes digitales ou de la rétine ou bien encore la forme de la main. L'utilisation de tels renseignements personnels à des fins d'identification, bien que rare actuellement, sauf peut-être en matière criminelle, nous incite à une élémentaire prudence.

Le recours à cette nouvelle technologie devrait en effet être sévèrement encadré par le législateur, surtout afin que soit préservée l'intégrité physique des personnes et soit évitée la création de banque de données nominatives à ce sujet.

De l'avis de la Commission, l'avant-projet de loi édicte des règles qui manifestement limiteraient les effets indésirables de l'utilisation de la biométrie à des fins d'identification : ce sont les conditions que l'on retrouve à l'article 50 et qui pourrait se résumer ainsi :

- Nul ne peut exiger que la vérification ou la confirmation de l'identité d'une personne soit faite au moyen d'un procédé permettant de saisir des caractéristiques ou des mesures biométriques.
- Que la volonté de la personne, c'est-à-dire son consentement, puisse être pris en compte afin que son identité soit établie par la biométrie.
- Réduire au minimum le nombre de données biométriques nécessaires à l'identification.
- Que les renseignements biométriques recueillis ne servent qu'aux fins de l'identification.
- Ces renseignements biométriques doivent être détruits lorsque l'objet pour lequel ils ont été recueillis est accompli, soit l'identification.
- La création d'une banque de données biométriques doit être divulguée à la Commission.

Dans la mesure où toutes les conditions qui y sont prévues seraient rendues obligatoires, la Commission n'entend pas s'opposer à la cueillette de renseignements biométriques.

Toutefois, au sujet de la dernière condition énumérée à l'article 50 de l'avant-projet de loi, soit celle qui énonce l'obligation de divulguer la création d'une banque de renseignements biométriques, la Commission croit qu'il serait plus appropriée que son intervention puisse se faire *a priori*, c'est-à-dire avant que la banque de caractéristiques ou de mesures biométriques ne soit créée. Une telle intervention préalable lui permettrait de s'assurer du respect des conditions de l'article 50.

De plus, la Commission estime que le pouvoir d'ordonnance qui lui est reconnu par cet article 50 devrait également couvrir la communication des banques de données biométriques et non seulement leur confection, leur utilisation, leur consultation ou leur conservation. En effet, la meilleure protection qui pourrait être offerte aux individus à ce sujet serait de restreindre considérablement la possibilité qu'auraient les organismes publics de pouvoir se communiquer entre eux de telles banques de données.

II.4 LES DOCUMENTS TECHNOLOGIQUES : CONDITIONS DE CONSERVATION ET D'ACCÈS

En dernier lieu, nous faisons trois recommandations visant à renforcer la sécurité et la confidentialité dans lesquelles on conserve les documents technologiques.

Premièrement, il est primordial pour la vie démocratique que toute atteinte à la vie privée soit la moins intrusive possible et qu'elle se fasse en stricte conformité avec la loi. Un intermédiaire de service n'a pas l'obligation de contrôler les activités afin de déceler celles qui pourraient être illicites. Et inversement, intercepter du courrier électronique ou lire des documents de quelqu'un sous enquête par les forces de la sécurité publique ne doit se faire qu'en stricte conformité avec les principes du Code criminel. Nous espérons que c'est la seule interprétation possible du 2e alinéa de l'article 30.

Dans le même ordre d'idées, pour une plus grande certitude juridique, la Commission croit que l'on pourrait préciser le rôle et les obligations des intermédiaires de service en vertu de la *Loi d'accès* et de la *Loi sur le secteur privé*.

Finalement, la consultation à distance des documents d'organismes publics permettrait un plus grand accès à l'information pour les citoyens. Toutefois, une telle consultation devra se faire, au préalable, en assurant la sécurité et la confidentialité.

III. CONCLUSION

Pour terminer, la Commission souligne son appui à cette initiative qui aurait, croit-elle, l'effet, entre autres, de clarifier l'application des principes contenus à la *Loi d'accès* et la *Loi sur le secteur privé* dans le contexte des supports technologiques en évolution constante. Pour cette raison, elle souhaite que l'avant-projet puisse être traduit en projet de loi dans un avenir rapproché.

Toutefois, elle souligne les dangers à la vie privée qui existent pour les citoyens si ces nouveaux modes de communication ne sont pas balisés adéquatement dès le début de leur utilisation.

Politique de confidentialité | Copyrights